Title (en)

Method and circuit for countermeasures to protect data present in an electronic circuit

Title (de)

Verfahren und Schaltkreis zur Gegenabwehr zum Schutz von Daten in einem elektronischen Schaltkreis

Title (fr)

Procédé et dispositif de contremesure pour protéger des données circulant dans un composant électronique

Publication

EP 2343806 A1 20110713 (FR)

Application

EP 10015368 A 20101207

Priority

FR 0906352 A 20091224

Abstract (en)

The method involves supplying data to process the inputs (A1-A4) of a logic circuit during a data processing phase, and supplying a precharge command signal (P) launching a precharge phase on input of the logic circuit. The functioning of logic gates (AG1, AG2, OG1, OG2) e.g. AND, NAND, OR, or NOR type gate, of a statistically unbalanced logic circuit is adopted, so that the output signal of the logic gate is in a binary state with a same probability as the random binary data supplied on input of the logic circuit during the precharge phase. An independent claim is also included for a device for a countermeasure method for a logic circuit to protect sensitive data processed in an electronic component of a portable device comprising a multiplexer.

Abstract (fr)

L'invention concerne un de contremesure dans un circuit logique comprenant une porte logique (OG1, OG2, AG1, AG2) fournissant un signal de sortie binaire (S), le procédé comprenant des étapes de fourniture de données binaires ayant des valeurs aléatoires à des entrées (A1-A4) du circuit logique durant une phase de précharge, de fourniture de données à traiter aux entrées du circuit logique durant une phase de traitement de données, de fourniture en entrée du circuit logique d'un signal de commande de précharge (P) déclenchant une phase de précharge, et sous l'effet du signal de commande de précharge, d'adaptation du fonctionnement d'une porte logique (OG10, AG10, LG) du circuit logique, non équilibrée statistiquement, pour que le signal sortie (S) de la porte logique soit dans un état binaire avec une même probabilité que les données binaires aléatoires fournies en entrée du circuit logique durant la phase de précharge.

IPC 8 full level

H03K 19/003 (2006.01)

CPC (source: EP US)

H03K 19/003 (2013.01 - EP US)

Citation (search report)

- [A] WO 0155821 A2 20010802 - ANDERSON ROSS JOHN [GB], et al
- [A] DE 10344647 B3 20050217 - INFINEON TECHNOLOGIES AG [DE]
- [A] US 6133761 A 20001017 - MATSUBARA GENSOH [JP]
- [A] DE 102005037355 B3 20061207 - INFINEON TECHNOLOGIES AG [DE]

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 2343806 A1 20110713; **EP 2343806 B1 20120718**; FR 2954868 A1 20110701; US 2011156756 A1 20110630; US 2013002302 A1 20130103; US 8330495 B2 20121211; US 9077334 B2 20150707

DOCDB simple family (application)

EP 10015368 A 20101207; FR 0906352 A 20091224; US 201213608904 A 20120910; US 97339110 A 20101220